EXHIBIT A

Bruce Schneier

Contact: schneier@schneier.com

Background

Bruce Schneier is an internationally renowned security technologist, called a "security guru" by the *Economist*. He is the *New York Times* best-selling author of 16 books—including his latest, *A Hacker's Mind*—as well as hundreds of articles, essays, and academic papers. His influential newsletter *Crypto-Gram* and blog *Schneier on Security* are read by over 250,000 people. Schneier is a fellow at the Berkman-Klein Center for Internet and Society at Harvard University; a Lecturer in Public Policy at the Harvard Kennedy School; a board member of the Electronic Frontier Foundation, AccessNow, and the Tor Project; and an advisory board member of EPIC and VerifiedVoting.org. He is the Chief of Security Architecture at Inrupt, Inc.

Professional Experience

2019–present, Chief of Security Architecture, Inrupt, Inc., Boston, MA.

2016–2019, Chief Technology Officer, IBM Resilient, and special advisor to IBM Security, Cambridge, MA.

2014–2016, Chief Technology Officer, Resilient Systems, Inc. (formerly called Co3 Systems, Inc.), Cambridge, MA.

2006–2013, Chief Security Technology Officer, British Telecom, London, UK.

1999–2006, Chief Technology Officer, Counterpane Internet Security, Inc., Cupertino, CA.

1993–1999, President, Counterpane Systems, Oak Park, IL and Minneapolis, MN.

1991–1993, Member of Technical Staff, AT&T Bell Labs., Schaumburg, IL.

1990, Director of Operations, Intelligent Resources Information Systems, Inc., Chicago, IL.

1987–1990, Program Manager, Space and Naval Warfare Systems Command, Arlington, VA.

1984–1987, Electronics Engineer, Naval Electronics Systems Security Engineering Center, Washington, DC.

Academic Experience

2016+, Lecturer in Public Policy, John F. Kennedy School of Government, Harvard University.

2016–2018, Research Fellow in the Science, Technology, and Public Policy program at the Belfer Center for Science and International Affairs, Kennedy School of Government, Harvard University.

2013+, Fellow and Faculty Associate, Berkman Klein Center for Internet and Society, Harvard University.

Board Membership

2017+, Board Member, AccessNow, New York, NY

2013+, Board Member, Electronic Frontier Foundation, San Francisco, CA.

2016–2021, Board Member, Tor Project, Cambridge, MA.

2004–2013, Board Member, Electronic Privacy Information Center, Washington DC.

Education

MS Computer Science, American University, 1986.

BS Physics, University of Rochester, 1984.

Books

AI and the New Future of Democracy: Changes in Politics, Legislating, Bureaucracy, Courtrooms, and Citizens (with Nathan Sanders), MIT Press, Fall 2025 (forthcoming).

A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend Them Back, WW Norton & Co., 2023.

We Have Root: Even More Advice from Schneier on Security, John Wiley & Sons, 2019.

Click Here to Kill Everybody: Security and Survival in a Hyper-connected World, WW Norton & Co., 2018.

Data and Goliath: The Hidden Battles to Capture Your Data and Control Your World, WW Norton & Co,, 2015.

Carry On: Sound Advice from Schneier on Security, John Wiley & Sons, 2013.

Liars and Outliers: Enabling the Trust that Society Needs to Thrive, John Wiley & Sons, 2012.

Cryptography Engineering (with Niels Ferguson and Tadayoshi Kohno), John Wiley & Sons, 2010.

Schneier on Security, John Wiley & Sons, 2008.

Beyond Fear: Thinking Sensibly about Security in an Uncertain World, Copernicus Books, 2003.

Practical Cryptography (with Niels Ferguson), John Wiley & Sons, 2003

Secrets & Lies: Digital Security in a Networked World, John Wiley & Sons, 2000.

The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance (with David Banisar), John Wiley & Sons, 1997.

Applied Cryptography, Second Edition, John Wiley & Sons, 1996.

The Twofish Encryption Algorithm (with John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson), John Wiley & Sons, 1996.

E-Mail Security, John Wiley & Sons, 1995

Protect Your Macintosh, Peachpit Press, 1994

Applied Cryptography, John Wiley & Sons, 1994.

Academic Publications

C. Summerfield, L. Argyle, M. Bakker, T. Collins, E. Durmus, T. Eloundou, I. Gabriel, D. Ganguli, K. Hackenburg, G. Hadfield, L. Hewitt, S. Huang, H. Landemore, N. Marchal, A. Ovadya, A. Procaccia, M. Risse, B. Schneier, E. Seger, D. Siddarth, H. S. Sætra, M. H. Tessler, M. Botvinick, "How Will Advanced AI Systems Impact Democracy?," arXiv:2409.06729 [cs.CY], August 27, 2024.

C. Porios, L. Guerin, and B. Schneier, "Assessing the Neutrality of Edits on Wikipedia," Wiki Workshop (11th edition), June 20, 2024.

F. Heiding, B. Schneier, and A. Vishwanath, "AI Will Increase the Quantity—and Quality—of Phishing Scams," *Harvard Business Review*, May 30, 2024.

F. Heiding, B. Schneier, A. Vishwanath, J. Bernstein, P. S. Park, "Devising and Detecting Phishing Emails Using Large Language Models," *IEEE Access*, March 11, 2024.

B. Raghavan and B. Schneier, "A Bold New Plan for Preserving Online Privacy and Security: Decoupling Our Identities from Our Data and Actions Could Safeguard Our Secrets," *IEEE Spectrum*, December 2023.

Bruce Schneier CV: Academic Publications   **4**

N. E. Sanders, A. Ulinich, and B. Schneier, "Demonstrations of the Potential of AI-based Political Issue Polling," arXiv:2307.04781 [cs.CY], July 10, 2023.

J. Penney and B. Schneier, "Platforms, Encryption, and the CFAA: The Case of *WhatsApp v. NSO Group*," *Berkeley Technology Law Journal*, v. 36, n. 1, 2021.

H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, J. Callas, W. Diffie, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier, V. Teague, C. Troncoso, "Bugs in our Pockets: The Risks of Client-Side Scanning," arXiv:2110.07450 [cs.CR], October 14, 2021.

N. E. Sanders and B. Schneier, "Machine Learning Featurizations for AI Hacking of Political Systems," arXiv:2110.09231 [cs.CY], October 8, 2021.

H. Farrell and B. Schneier, "Rechanneling Beliefs: How Information Flows Hinder or Help Democracy," Stavros Niarchos Foundation SNF Agora Institute, Johns Hopkins, May 24, 2021.

B. Schneier, "The Coming AI Hackers," Belfer Center for Science and International Affairs, Harvard Kennedy School, April 2021.

G. Corn, J. Daskal, J. Goldsmith, C. Inglis, P. Rozenzweig, S. Sacks, B. Schneier, A. Stamos, V. Stewart, "Chinese Technology Platforms Operating in the United States: Assessing the Threat," *Joint Report of the National Security, Technology, and Law Working Group at the Hoover Institution at Stanford University and the Tech, Law & Security Program at American University Washington College of Law*, February 11, 2021.

R. S. S. Kumar, J. Penney, B. Schneier, K. Albert, "Legal Risks of Adversarial Machine Learning Research," arXiv:2006.16179.

N. Kim, T. Herr, and B. Schneier, "The Reverse Cascade: Enforcing Security on the Global IoT Supply Chain," *Atlantic Council*, June 2020.

K. Levy and B. Schneier, "Privacy Threats in Intimate Relationships," *Journal of Cybersecurity*, v. 6, n. 1, 2020.

M. Bourdeaux, G. Abiola, B. Edgar, J. Pershing J. Wang, M. Van Loon, B. Schneier, "Weaponizing Digital Health Intelligence," *Belfer Center for Science and International Affairs, Harvard Kennedy School*, January 2020.

K. Albert, J. Penney, B. Schneier, R. Shankar, and S. Kumar, "Politics of Adversarial Machine Learning," *arXiv:2002.05648*, February 2020.

A. Adams, F. Ben-Youssef, B. Schneier, K. Murata, "Superheroes on Screen: Real Life Lessons for Security Debates," *Security Journal*, 2019.

H. Farrell, B. Schneier, "Common-Knowledge Attacks on Democracy," Berkman Klein Center Research Publication No. 2018-7, October 2018.

Bruce Schneier CV: Published Articles   5

T. Herr, B. Schneier, and C. Morris, "Taking Stock: Estimating Vulnerability Rediscovery," July 2017 (revised October 2017).

O. S. Kerr, B. Schneier, "Encryption Workarounds," March 2017.

S. Shackelford, B. Schneier, M. Sulmeyer, A. Boustead, B. Buchanan, A. Craig, T. Herr, and J. Z. Malekos Smith, "Making Democracy Harder to Hack: Should Elections Be Classified as 'Critical Infrastructure'?," *University of Michigan Journal of Law Reform*, v. 50, n. 3, Spring 2017, pp. 629–668.

J. Quinn and B. Schneier, "A Proportional Voting System for Awards Nominations Resistant to Voting Blocs," *Voting Matters*, n. 31, to appear.

B. Schneier, K. Seidel, S. Vijayakumar, "A Worldwide Survey of Encryption Products," Berkman Center Report, February 11, 2016.

U. Gasser, M. G. Olsen, N. Gertner, D. Renan, J. Goldsmith, J. Sanchez, S. Landau, B. Schneier, J. Nye, L. Schwartztol, D. R. O'Brien, J. Zittrain, "Don't Panic: Making Progress on the 'Going Dark' Debate," Berkman Center Report, February 1, 2016.

H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier, M. Specter, D. J. Weitzner, "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," *Journal of Cybersecurity,* November 2015.

B. Schneier, M. Fredrikson, T. Kohno, T. Ristenpart, "Surreptitiously Weakening Cryptographic Systems," *Cryptology ePrint Archive* Report 2015/097, 2015.

104 additional academic publications before January 2015.

Published Articles

"Trust Issues," *Boston Review*, December 6, 2024.

"The Apocalypse That Wasn't: AI Was Everywhere in 2024's Elections, but Deepfakes and Misinformation Were Only Part of the Picture," *The Conversation*, December 4, 2024.

"Algorithms Are Coming for Democracy—but It's Not All Bad," *Wired*, November 27, 2024.

"The SEC Whistleblower Program Is Dominating Regulatory Enforcement," *The American Prospect*, October 18, 2024.

"AI Could Still Wreck the Presidential Election," The Atlantic, September 27, 2024.

"Israel's Pager Attacks Have Changed the World," The New York TImes, September 22, 2024.

Bruce Schneier CV: Published Articles   **6**

"Let's Start Treating Cybersecurity Like It Matters," Defense One, August 2, 2024.

"The CrowdStrike Outage and Market-Driven Brittleness," Lawfare, July 25, 2024.

"The Hacking of Culture and the Creation of Socio-Technical Debt," *e-flux*, June 18, 2024.

"Using AI for Political Polling," *Harvard Kennedy School Ash Center*, June 11, 2024.

"Indian Election Was Awash in Deepfakes—but AI Was a Net Positive for Democracy," *The Conversation*, June 7, 2024.

"How Online Privacy Is Like Fishing," *IEEE Spectrum*, June 4, 2024.

"How AI Will Change Democracy," *Cyberscoop*, May 28, 2024.

"Seeing Like a Data Structure," *Harvard Kennedy School Belfer Center*, May 25, 2024.

"Lattice-Based Cryptosystems and Quantum Cryptanalysis," *Communications of the ACM*, May 25, 2024.

"LLMs' Data-Control Path Insecurity," *Communications of the ACM*, May 12, 2024.

"AI and Trust," *The Herald Business*, April 30, 2024.

"It's the End of the Web as We Know It," *The Atlantic*, April 24, 2024.

"Backdoor in XZ Utils That Almost Happened," *Lawfare*, April 9, 2024.

"In Memoriam: Ross Anderson, 1956-2024," *Communications of the ACM*, April 9, 2024.

"Public AI as an Alternative to Corporate AI," *New America*, March 14, 2024.

"Let's Not Make the Same Mistakes with AI That We Made with Social Media," *MIT Technology Review*, March 13, 2024.

"How Public AI Can Strengthen Democracy," *Brookings*, March 4, 2024.

"How the 'Frontier' Became the Slogan of Uncontrolled AI," *Jacobin*, February 28, 2024.

"Building a Cyber Insurance Backstop Is Harder Than It Sounds," *Lawfare*, February 26, 2024.

"CFPB's Proposed Data Rules Would Improve Security, Privacy and Competition," *Cyberscoop*, January 26, 2024.

"Don't Talk to People Like They're Chatbots," *Atlantic*, January 17, 2024.

"AI Needs to Be Both Trusted and Trustworthy," *Wired*, January 1, 2024.

Bruce Schneier CV: Published Articles   7

"AI Could Improve Your Life by Removing Bottlenecks between What You Want and What You Get," *The Conversation*, December 21, 2023.

"The Internet Enabled Mass Surveillance. AI Will Enable Mass Spying," *Slate*, December 4, 2023.

"AI and Trust," *Harvard Kennedy School Belfer Center*, December 1, 2023.

"Ten Ways AI Will Change Democracy," *Harvard Kennedy School Ash Center*, November 6, 2023.

"Trustworthy AI Means Public AI," *IEEE Security & Privacy*, November 1, 2023.

"Who's Accountable for AI Usage in Digital Campaign Ads? Right Now, No One," *Harvard Kennedy School Ash Center*, October 11, 2023.

"AI Disinformation Is a Threat to Elections—Learning to Spot Russian, Chinese and Iranian Meddling in Other Countries Can Help the Us Prepare for 2024," *The Conversation*, September 29, 2023.

"The A.I. Wars Have Three Factions, and They All Crave Power," *New York Times*, September 28, 2023.

"Robots Are Already Killing People," *Atlantic*, September 6, 2023.

"Nervous About ChatGPT? Try ChatGPT With a Hammer," *Wired*, August 29, 2023.

"Re-Imagining Democracy for the 21st Century, Possibly Without the Trappings of the 18th Century," *The Conversation*, August 7, 2023.

"Six Ways That AI Could Change Politics," *MIT Technology Review*, July 28, 2023.

"Can You Trust AI? Here's Why You Shouldn't," *The Conversation*, July 20, 2023.

"AI Microdirectives Could Soon Be Used for Law Enforcement," *Slate*, July 17, 2023.

"Will AI Hack Our Democracy?," *Harvard Kennedy School Magazine*, July 14, 2023.

"Snowden Ten Years Later," *RFC 9446*, July 1, 2023.

"Artificial Intelligence Can't Work Without Our Data," *Politico*, June 29, 2023.

"AI Could Shore Up Democracy—Here's One Way," *The Conversation*, June 20, 2023.

"Build AI by the People, for the People," *Foreign Policy*, June 12, 2023.

 "Big Tech Isn't Prepared for A.I.'s Next Chapter," *Slate*, May 30, 2023.

"Rethinking Democracy for the Age of AI," *Cyberscoop*, May 10, 2023.

"Can We Build Trustworthy AI?," *Gizmodo*, May 4, 2023.

Bruce Schneier CV: Published Articles   **8**

"Just Wait Until Trump Is a Chatbot," *The Atlantic*, April 28, 2023.

"How Artificial Intelligence Can Aid Democracy," *Slate*, April 21, 2023.

"Brace Yourself for a Tidal Wave of ChatGPT Email Scams," *Wired*, April 4, 2023.

"How AI Could Write Our Laws," *MIT Technology Review*, March 14, 2023.

"Why the U.S. Should Not Ban TikTok," *Foreign Policy*, February 23, 2023.

"Everything Is Hackable," *Slate*, February 10, 2023.

"We Don't Need to Reinvent Our Democracy to Save It from AI," *Harvard Kennedy School Belfer Center*, February 9, 2023.

"The Big Idea: Bruce Schneier," *Whatever*, February 7, 2023.

"Opinion: What Peter Thiel and the 'Pudding Guy' revealed," *CNN*, February 7, 2023.

"How ChatGPT Hijacks Democracy," *New York Times*, January 15, 2023.

"How to Decarbonize Crypto," *Atlantic*, December 6, 2022.

"Centralized vs. Decentralized Data Systems—Which Choice Is Best?" *VentureBeat*, September 12, 2022.

"NIST's Post-Quantum Cryptography Standards Competition," *IEEE Security & Privacy*, August 7, 2022.

"When Corporate Interests and International Cyber Agreements Collide," *Cipher Brief*, May 5, 2022.

"Why Vaccine Cards Are So Easily Forged," *The Atlantic*, March 8, 2022.

"Letter to the US Senate Judiciary Committee on App Stores," January 31, 2022.

"Robot Hacking Games," *IEEE Security & Privacy*, January 1, 2022.

"How to Cut Down on Ransomware Attacks Without Banning Bitcoin," *Slate*, June 17, 2021.

"Hacked Drones and Busted Logistics Are the Cyber Future of Warfare," *Brookings TechStream*, June 5, 2021.

"Russia's Hacking Success Shows How Vulnerable the Cloud Is," *Foreign Policy*, May 24, 2021.

"'Grassroots' Bot Campaigns Are Coming. Governments Don't Have a Plan to Stop Them.," *The Washington Post*, May 20, 2021.

"Hackers Used to Be Humans. Soon, AIs Will Hack Humanity," *Wired*, April 19, 2021.

Bruce Schneier CV: Published Articles   **9**

"Bitcoin's Greatest Feature Is Also Its Existential Threat," *Wired*, March 9, 2021.

"Illuminating SolarStorm: Implications for National Strategy and Policy," *Aspen Institute*, March 04, 2021.

"Why Was SolarWinds So Vulnerable to a Hack?" *New York Times*, February 23, 2021.

"The Government Will Guard Biden's Peloton from Hackers. What About the Rest of Us?," *The Washington Post*, February 2, 2021.

"The Solarwinds Hack Is Stunning. Here's What Should Be Done," *CNN*, January 5, 2021.

"Audio: Firewalls Don't Stop Dragons Podcast," *Firewalls Don't Stop Dragons*, December 28, 2020.

"Audio: The Hack by Russia Is Huge. Here's Why It Matters.," *MPR News*, December 28, 2020.

"Review of Data and Goliath (German)," *Nerdhalla*, December 27, 2020.

"Video: The Most Consequential Cyber-Attack in History Just Happened. What Now?," *LA Times*, December 24, 2020.

"Video: AshbrookLIVE #14 – Bruce Schneier," *AshbrookLIVE*, December 24, 2020.

"Audio: Full Disclosure with Bruce Schneier," *BarCode*, December 20, 2020.

"Audio: How Your Digital Footprint Makes You the Product," *TechSequences*, December 16, 2020.

"Video: Hack in the Box Security Conference Keynote Interview," *Hack In The Box Security Conference*, December 3, 2020.

"Video: Election Security: Securing the Vote While Securing the System," *The Legal Edition*, November 19, 2020.

"#ISC2Congress: Modern Security Pros Are Much More than Technologists, Says Bruce Schneier," *Infosecurity*, November 18, 2020.

"Audio: Ballot Question 1: Risks & Regulations Regarding Right to Repair," *Pioneer Institute*, October 13, 2020.

"Audio: We Live in a Security and Privacy World that Science Fiction Didn't Predict," *OWASP PDX Podcast*, October 4, 2020.

"How Amazon and Walmart Could Fix IoT Security," *Data Breach Today*, June 26, 2020.

"The Cyberflâneur #29: Bruce Schneier," *The Syllabus*, June 16, 2020.

Bruce Schneier CV: Published Articles   **10**

"Audio: Interview with Bruce Schneier for Blockchain Rules Podcast Series," *Blockchain Rules Podcast*, June 16, 2020.

"Audio: Is Contact Tracing Dumb? False Positives, Loss of Trust, and an Uncertain Path Back to Normalcy," *Policy Punchline*, June 2, 2020.

"Coronavirus, il guru Bruce Schneier: «Le app di contact tracing? Inutili. Margini di errore troppo alti»," *Open*, June 2, 2020.

"Audio: Click Here to Kill Everybody: Security and Survival in a Hyper-connected World," *Policy Punchline*, May 29, 2020.

"Audio: Bruce Schneier on Truth, Reality, and Contact Tracing," *Reality 2.0*, May 27, 2020.

"Video: Public Interest Technologists—Interview with Bruce Schneier and Jon Callas," *Cyber Cyber Cyber Cyber*, May 19, 2020.

"The Public Good Requires Private Data," *Foreign Policy*, May 16, 2020.

"How Hackers and Spies Could Sabotage the Coronavirus Fight," *Foreign Policy*, February 28, 2020.

"Technologists vs. Policy Makers," *IEEE Security & Privacy*, January/February 2020.

"We're Banning Facial Recognition. We're Missing the Point.," *The New York Times*, January 20, 2020.

"China Isn't the Only Problem With 5G," *Foreign Policy*, January 10, 2020.

"Bots Are Destroying Political Discourse As We Know It," *The Atlantic*, January 7, 2020.

"We Must Bridge the Gap Between Technology and Policymaking. Our Future Depends on It," *World Economic Forum*, November 12, 2019.

"Every Part of the Supply Chain Can Be Attacked," *The New York Times*, September 25, 2019.

"The Real Threat from China Isn't 'Spy Trains,'" *CNN*, September 21, 2019.

"What Digital Nerds and Bio Geeks Have to Worry About," *CNN*, September 13, 2019.

"The Myth of Consumer Security," *Lawfare*, August 26, 2019.

"8 Ways to Stay Ahead of Influence Operations," *Foreign Policy*, August 12, 2019.

"Attorney General William Barr on Encryption Policy," *Lawfare*, July 23, 2019.

"We Must Prepare for the Next Pandemic," *The New York Times*, June 17, 2019.

Bruce Schneier CV: Published Articles **11**

"AI Has Made Video Surveillance Automated and Terrifying," *Motherboard*, June 13, 2019.

"AI Can Thrive in Open Societies," *Foreign Policy*, June 13, 2019.

"When Fake News Comes to Academia," *Lawfare*, May 24, 2019.

"Democracy's Dilemma," *Boston Review*, May 15, 2019.

"Russia's Attacks on Our Democratic Systems Call for Diverse Countermeasures," *The Hill*, May 7, 2019.

"Toward an Information Operations Kill Chain," *Lawfare*, April 24, 2019.

"A New Privacy Constitution for Facebook," *OneZero*, March 8, 2019.

"Cybersecurity for the Public Interest," *IEEE Security & Privacy*, January/February 2019.

"There's No Good Reason to Trust Blockchain Technology," *Wired*, February 6, 2019.

"The Public-Interest Technologist Track at the RSA Conference," *RSA Conference Blogs*, January 29, 2019.

"Defending Democratic Mechanisms and Institutions against Information Attacks," *Defusing Disinfo*, January 28, 2019.

"Evaluating the GCHQ Exceptional Access Proposal," *Lawfare*, January 17, 2019.

"Machine Learning Will Transform How We Detect Software Vulnerabilities," *SecurityIntelligence*, December 18, 2018.

"The Most Damaging Election Disinformation Campaign Came From Donald Trump, Not Russia," *Motherboard*, November 19, 2018.

"Surveillance Kills Freedom By Killing Experimentation," *Wired*, November 16, 2018.

"Information Attacks on Democracies," *Lawfare*, November 15, 2018.

"We Need Stronger Cybersecurity Laws for the Internet of Things," *CNN*, November 9, 2018.

"Nobody's Cellphone Is Really That Secure," *The Atlantic*, October 26, 2018.

"Internet Hacking Is About to Get Much Worse," *New York Times*, October 11, 2018.

"Cryptography after the Aliens Land," *IEEE Security & Privacy*, September/October 2018.

"Don't Fear the TSA Cutting Airport Security. Be Glad That They're Talking about It," *Washington Post*, August 17, 2018.

"Censorship in the Age of Large Cloud Providers," *Lawfare*, June 7, 2018.

"Why the FBI Wants You to Reboot Your Router — and Why That Won't Be Enough Next Time," *The Washington Post*, June 6, 2018.

"Data Protection Laws Are Shining a Needed Light on a Secretive Industry," *The Guardian*, June 1, 2018.

"What 'Efail' Tells Us About Email Vulnerabilities and Disclosure," *Lawfare*, May 24, 2018.

"Banning Chinese Phones Won't Fix Security Problems with Our Electronic Supply Chain," *The Washington Post*, May 8, 2018.

"American Elections Are Too Easy to Hack. We Must Take Action Now," *The Guardian*, April 18, 2018.

"It's Not Just Facebook. Thousands of Companies are Spying on You," *CNN*, March 26, 2018.

"Artificial Intelligence and the Attack/Defense Balance," *IEEE Security & Privacy*, March/April 2018.

"Can Consumers' Online Data Be Protected?," *CQ Researcher*, February 9, 2018.

"How to Fight Mass Surveillance Even Though Congress Just Reauthorized It," *The Washington Post*, January 25, 2018.

"The New Way Your Computer Can Be Attacked," *The Atlantic*, January 22, 2018.

"The Security of Pretty Much Every Computer on the Planet Has Just Gotten a Lot Worse," *CNN*, January 5, 2018.

"How the Supreme Court Could Keep Police From Using Your Cellphone to Spy on You," *The Washington Post*, November 27, 2017.

"Testimony Before the House Subcommittee on Digital Commerce and Consumer Protection," , November 1, 2017.

"Don't Waste Your Breath Complaining to Equifax about Data Breach ," *CNN*, September 11, 2017.

"IoT Security: What's Plan B?," *IEEE Security & Privacy*, September/October 2017.

"'Twitter and Tear Gas' Looks at How Protest Is Fueled and Crushed by the Internet," *Motherboard*, July 11, 2017.

"Why the NSA Makes Us More Vulnerable to Cyberattacks," *Foreign Affairs*, May 30, 2017.

Bruce Schneier CV: Published Articles   **13**

"Who Are the Shadow Brokers?," *The Atlantic*, May 23, 2017.

"What Happens When Your Car Gets Hacked?," *The New York Times*, May 19, 2017.

"Why Extending Laptop Ban Makes No Sense," *CNN*, May 16, 2017.

"The Next Ransomware Attack Will Be Worse than WannaCry," *The Washington Post*, May 16, 2017.

"Three Lines of Defense against Ransomware Attacks," *New York Daily News*, May 15, 2017.

"Online Voting Won't Save Democracy," *The Atlantic*, May 10, 2017.

"Who Is Publishing NSA and CIA Secrets, and Why?," *Lawfare*, April 27, 2017.

"The Quick vs the Strong: Commentary on Cory Doctorow's *Walkaway*," *Crooked Timber*, April 26, 2017.

"Infrastructure Vulnerabilities Make Surveillance Easy," *Al Jazeera*, April 11, 2017.

"Snoops May Soon Be Able to Buy Your Browsing History. Thank the US Congress," *The Guardian*, March 30, 2017.

"Puzzling out TSA's Laptop Travel Ban," *CNN*, March 22, 2017.

"Security Orchestration for an Uncertain World," *SecurityIntelligence*, March 21, 2017.

"How to Keep Your Private Conversations Private for Real," *The Washington Post*, March 8, 2017.

"Botnets of Things," *MIT Technology Review*, March/April 2017.

"Click Here to Kill Everyone," *New York Magazine*, January 27, 2017.

"Why Proving the Source of a Cyberattack is So Damn Difficult," *CNN*, January 5, 2017.

"Class Breaks," *Edge*, December 30, 2016.

"U.S. Elections Are a Mess, Even Though There's No Evidence This One Was Hacked," *The Washington Post*, November 23, 2016.

"Testimony at the U.S. House of Representatives Joint Hearing 'Understanding the Role of Connected Devices in Recent Cyber Attacks,'" November 16, 2016.

"American Elections Will Be Hacked," *The New York Times*, November 9, 2016.

"Your WiFi-Connected Thermostat Can Take Down the Whole Internet. We Need New Regulations.," *The Washington Post*, November 3, 2016.

"Lessons From the Dyn DDoS Attack," *SecurityIntelligence*, November 1, 2016.

Bruce Schneier CV: Published Articles   **14**

"Cybersecurity Issues for the Next Administration," *Time*, October 13, 2016.

"We Need to Save the Internet from the Internet of Things," *Motherboard*, October 6, 2016.

"How Long Until Hackers Start Faking Leaked Documents?," *The Atlantic*, September 13, 2016.

"Someone Is Learning How to Take Down the Internet," *Lawfare*, September 13, 2016.

"Stop Trying to Fix the User," *IEEE Security & Privacy*, September/October 2016.

"New Leaks Prove It: The NSA Is Putting Us All at Risk to Be Hacked," *Vox*, August 24, 2016.

"Hackers Are Putting U.S. Election at Risk," *CNN*, July 28, 2016.

"By November, Russian Hackers Could Target Voting Machines," *The Washington Post*, July 27, 2016.

"The Internet of Things Will Turn Large-Scale Hacks into Real World Disasters," *Motherboard*, July 25, 2016.

"Credential Stealing as Attack Vector," *Xconomy*, April 20, 2016.

"The Value of Encryption," *The Ripon Forum*, April 2016.

"Can You Trust IRS to Keep Your Tax Data Secure?," *CNN*, April 13, 2016.

"Your iPhone Just Got Less Secure. Blame the FBI.," *The Washington Post*, March 29, 2016.

"Cryptography Is Harder Than It Looks," *IEEE Security & Privacy*, January/February 2016.

"Data Is a Toxic Asset, So Why Not Throw It Out?," *CNN*, March 1, 2016.

"A 'Key' for Encryption, Even for Good Reasons, Weakens Security," *The New York Times Room for Debate*, February 23, 2016.

"Why You Should Side With Apple, Not the FBI, in the San Bernardino iPhone Case," *The Washington Post*, February 18, 2016.

"Candidates Won't Hesitate to Use Manipulative Advertising to Score Votes," *The Guardian*, February 4, 2016.

"The Internet Of Things Will Be The World's Biggest Robot," *Forbes*, February 2, 2016.

"Security vs. Surveillance," *Don't Panic: Making Progress on the 'Going Dark' Debate*, February 1, 2016.

Bruce Schneier CV: Published Articles   **15**

"When Hacking Could Enable Murder," *CNN*, January 26, 2016.

"How an Overreaction to Terrorism Can Hurt Cybersecurity," *MIT Technology Review*, January 25, 2016.

"The Internet of Things That Talk About You Behind Your Back," *Motherboard*, January 8, 2016.

"The Risks—and Benefits—of Letting Algorithms Judge Us," *CNN*, January 6, 2016.

"How the Internet of Things Limits Consumer Choice," *The Atlantic*, December 24, 2015.

"Can Laws Keep Up with Tech World?," *CNN*, December 21, 2015.

"The Automation of Reputation," *Edge.org*, November 5, 2015.

"The Rise of Political Doxing," *Motherboard*, October 28, 2015.

"Face Facts about Internet Security," *CNN*, October 23, 2015.

"The Era Of Automatic Facial Recognition And Surveillance Is Here, *Forbes*, September 29, 2015.

"Stealing Fingerprints," *Motherboard*, September 29, 2015.

"VW Scandal Could Just Be the Beginning," *CNN*, September 28, 2015.

"Living in Code Yellow," *Fusion*, September 22, 2015.

"Hacking Team, Computer Vulnerabilities, and the NSA," *Georgetown Journal of International Affairs*, September 13, 2015.

"Is It OK to Shoot Down a Drone over Your Backyard?" *CNN*, September 9, 2015.

"The Meanest Email You Ever Wrote, Searchable on the Internet," *Atlantic*, September 8, 2015.

"Should Some Secrets Be Exposed?" *CNN*, July 7, 2015.

"Why We Encrypt," Foreword to Privacy International's *Securing Safe Spaces Online*, June 2015.

"China and Russia Almost Definitely Have the Snowden Docs," *Wired,* June 16, 2015

"Why are We Spending $7 Billion on TSA?" *CNN,* June 5, 2015

"Debate: Should Companies Do Most of Their Computing in the Cloud?" *The Economist,* June 5, 2015

"How We Sold Our Souls—and More—to the Internet Giants," *The Guardian,* May 17, 2015

"Could Your Plane Be Hacked?" *CNN,* April 16, 2015

"Baseball's New Metal Detectors Won't Keep You Safe. They'll Just Make You Miss a Few Innings," *The Washington Post,* April 14, 2015

"The Big Idea: *Data and Goliath,*" *Whatever*, March 4, 2015.

"Hacker or Spy? In Today's Cyberattacks, Finding the Culprit Is a Troubling Puzzle," *The Christian Science Monitor*, March 4, 2015.

"The World's Most Sophisticated Hacks: Governments?," *Fortune*, March 3, 2015.

"Cyberweapons Have No Allegiance," *Motherboard*, February 25, 2015.

"Everyone Wants You To Have Security, But Not from Them," *Forbes*, February 23, 2015.

"Your TV May Be Watching You," *CNN*, February 11, 2015.

"When Thinking Machines Break The Law," *Edge*, January 28, 2015.

"The Importance of Deleting Old Stuff—Another Lesson From the Sony Attack," *Ars Technica*, January 12, 2015.

"The Government Must Show Us the Evidence That North Korea Attacked Sony," *Time*, January 5, 2015.

"We Still Don't Know Who Hacked Sony," *The Atlantic*, January 5, 2015.

435 additional published articles before October 2014.

Patents

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for educational testing," U.S. Patent 8,725,060, May 13, 2014.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for a cryptographically assisted commercial network system designed to facilitate buyer-driven conditional purchase offers," U.S. Patent 8,712,920, April 29, 2014.

J.S. Walker, B. Schneier, J.A. Jorasch, T.S. Case, "Conditional purchase offer management system," U.S. Patent 8,700,481, April 15, 2014.

J.S. Walker, B. Schneier, M.M Fincham, J.A. Jorasch, M.D. Downs, R.C. Tedesco, "Method and apparatus for promoting the selection and use of a transaction card," U.S. Patent 8,632,005, January 21, 2014.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for a cryptographically-assisted commercial network system designed to facilitate and support expert-based commerce," U.S. Patent 8,626,667, January 7, 2014.

77 additional patents before 2014.

Previous Declarations and Depositions

British Telecommunications PLC and BT Americas, Inc. v. Fortinet, Inc., In JAMS Arbitration, Case No. 5425002197. Testimony and trial as patent author (2025).

Academy LTD v. First Data Merchant Service, LLC, Case No. 2022-58352, District Court of Harris County, Texas, 11th Judicial District. Expert Witness for Academy, Yetter Coleman LPP, attorneys. Report (2024).

Anibal Rodriguez, Sal Cataldo, Julian Santiago, and Susan Lynn, individually and on behalf of all similarly situated v. Google LLC, Case No. 4:20-cv-04688-RS, United States District Court for the Northern California District. Expert witness for Brown et. al., Susman Godfrey LLP, attorneys. Declarations and deposition (2023).

Chasom Brown, William Byatt, Jeremy David, Christopher Castillo, and Monique Trujillo, individually and on behalf of all similarly situated v. Google LLC, Case No. 4:20-cv-03664-YGR-SVK, United States District Court for the Northern California District. Expert witness for Brown et. al., Susman Godfrey LLP, attorneys. Declarations and deposition (2022).

Mon Cheri Bridals, LLC and Maggie Sottero Designs, LLC v. Cloudflare, Inc., Case No. 2:18-cv-09453-MWF-AS, United States District Court for the Central District of California. Expert witness for Cloudflare, Inc., Fenwick & West, LLP, attorneys. Declarations (2020 and 2021).

Fortinet, Inc. v. BT Americas, Inc., Case No. IPR2019-01324, Inter Partes Review, United States Patent and Trademark Office before the Patent Trial and Appeal Board regarding U.S. Patent No. 7,895,641. Expert witness for BT Americas, Inc., Proskaur Rose LLP, attorneys. Declaration (2019).

United to Protect Democracy et al. v. Presidential Advisory Commission on Election Integrity et al., Civil Action No. 1:17-cv-02016, United States District Court for the District of Columbia. Declaration (2017).

Koninklijke Philips N.V. and U.S. Philips Corp. v. HTC Corp. and HT America, Civil Action No. 15-1126-GMS, United States District Court for the District of Delaware, concerning U.S. Patent Nos. 8.543.819 and 9.436.809. Expert witness for HTC Corp., Perkins Coie LLP, attorneys. Declaration (2017).

Ex parte reexamination of U.S. Patent No. 6,760,752. Expert witness for the patent holder Zix Corp., Haynes and Boone, LLC attorneys. Declaration (2017).

Great West Casualty Co., BITCO General Insurance Corp., and BITCO National Insurance Co. v. Transpacific IP Ltd, Case No. IPR2015-00x, Inter Partes Review, United States Patent and Trademark Office before the Patent Trial and Appeal Board regarding U.S. Patent No. 8,929,555. Expert witness for Great West Casualty Co.,

Bruce Schneier CV: Previous Declarations and Depositions   **18**

BITCO General Insurance Corp., and BITCO National Insurance Co., Sidley Austin LLP attorneys. Declaration (2015).

Unikey Technologies, Inc. v. Assa Abloy AB, Cases No. IPR2015-01440 and IPR2015-01441, Inter Partes Review, United States Patent and Trademark Office before the Patent Trial and Appeal Board regarding U.S. Patent Nos. 7,706,778 and 8,150,374. Expert witness for UniKey Technologies, Inc., Proskauer Rose LLP attorneys. Declaration (2015).

Epicor Software Corp. v. Protegrity Corp., Case Nos. CBM2015-00002 and CBM2015-00006, United States Patent and Trademark Office before the Patent Trial and Appeal Board regarding U.S. Patent Nos. 6,321,201 and 8,402.281. Expert witness for Epicor Software Corp., Cantor Colborn LLP attorneys. Declaration (2015) and deposition (2015).

Quantum World Corp. v. Dell, Inc. Civil Action No. A-11-CA-688-SS, United States District Court for the Western Division of Texas regarding U.S. Patent Nos. 6,763,364, 7,096,242, and 7,752,247. Expert witness for Dell, Inc., Alston & Bird attorneys. Declaration and deposition (2015).

Entrust, Inc. v. Secure Axcess, LLC, Case No. CBM2015-0027, Covered Business Method Review United States Patent and Trademark Office before the Patent Trial and Appeal Board concerning Patent No. 7,631,191. Expert witness for Entrust, Inc., Crowell & Morning LLP attorneys. Declaration (2014) and deposition (2015).

Apple, Inc. v. Achates Reference Publishing, Inc., Case Nos. IPR 13-00080 and IPR 13-00081, Inter Partes Review, United States Patent and Trademark Office before the Patent Trial and Appeal Board regarding U.S. Patent Nos. 6,173,403 and 5,982,889. Expert witness for Apple, Inc., DiNovo Price LLP and Sidley Austin LLP attorneys. Declaration and deposition.

Research in Motion Corp. v. Innovative Sonic, Docket No. 377211US, Inter Partes Review, United States Patent and Trademark Office regarding Patent No. 6,925,183. Expert witness for Research In Motion Corp., Expert witness for Research in Motion Corp., Oblon Spivak attorneys. Declaration.

Walker Digital, LLC v. MySpace, Inc., et al., Civil Action No. 1:11-cs-00318-LPS, United States District Court for the District of Delaware, concerning U.S. Patent Nos. 5,884,270 and 5,884,272. Deposition as patent author.

Walker Digital, LLC v. Google, Inc., et al., Civil Action No. 11-309-SLR, United States District Court for the District of Delaware, concerning U.S. Patent No. 5,768,382. Deposition as patent author.

TecSec, Inc. v. International Business Machines Corp., et al., Civil Action No. 1:10-cv-00115-LMB/TCB, United States District Court for the Eastern District of Virginia (Alexandria) concerning U.S. Patents No. 5,369,702 and 6,549,623. Expert witness for TecSec, Inc., Hunton & Williams LLP, attorneys for TecSec, Inc. Declaration and deposition.

Bruce Schneier CV: Previous Declarations and Depositions   **19**

Luciano F. Paone v. Microsoft Corp., Civil Action No. CV-07-2973 (E.D. NY), United States District Court for the Northern District of California concerning U.S. Patent No. 6,259,789. Expert witness for Microsoft Corp., Kirkland & Ellis attorneys. Declaration and deposition.

Fred and Kathleen Stark v. The Seattle Seahawks LLC, Civil Action No. CV-06-1719 JLR, United States District Court for the Western District of Washington at Seattle concerning the efficacy of pat-down searches. Expert witness for Stark, Danielson Harrigan Leyh & Tollefson LLC, attorneys for Stark. Declaration and deposition.

Gordon Johnston v. The Tampa Sports Authority et al., Civil Action No. 8-05-cv-02191-JDW-MAP, United States District Court for the Middle District of Florida Tampa Division. concerning the efficacy of pat-down searches. Expert witness for Johnston. Declaration.